INCIDENT RESPONSE

Per rispondere ai quesiti di CSIRT, iniziamo con la spiegazione delle tecniche richieste e la differenza tra Purge, Destroy e Clear per l'eliminazione delle informazioni sensibili.

I. Tecniche di Isolamento

Per isolare il sistema B infetto, si possono adottare le seguenti misure:

1. **Disconnessione dalla Rete**: Immediatamente scollegare il sistema B dalla rete interna (Rete Interna) e da Internet per prevenire ulteriori danni e fermare la comunicazione con l'attaccante.
2. **Segmentazione della Rete**: Implementare una segmentazione della rete per isolare il segmento compromesso e limitare il movimento laterale dell'attaccante.
3. **Controllo Accessi**: Modificare le regole del firewall per bloccare il traffico in entrata e in uscita verso e dal sistema B.
4. **Monitoraggio Costante**: Utilizzare sistemi di monitoraggio e logging per tracciare tutte le attività e capire meglio l'entità dell'attacco.

II. Tecniche di Rimozione del Sistema B Infetto

Per rimuovere il sistema B infetto, si possono seguire questi passaggi:

1. **Backup Sicuro**: Fare un backup dei dati essenziali presenti nel sistema B, assicurandosi che i backup siano sicuri e non compromessi.
2. **Spegnimento del Sistema**: Spegnere il sistema B per fermare qualsiasi attività dannosa.
3. **Rimozione Fisica**: Rimuovere fisicamente il sistema dal network per impedire qualsiasi accesso fisico o remoto.
4. **Sostituzione del Sistema**: Preparare un nuovo sistema pulito per sostituire quello infetto, garantendo che tutte le misure di sicurezza siano implementate.

Purge, Destroy e Clear

Per quanto riguarda l'eliminazione delle informazioni sensibili dai dischi compromessi, vediamo le differenze tra Purge, Destroy e Clear:

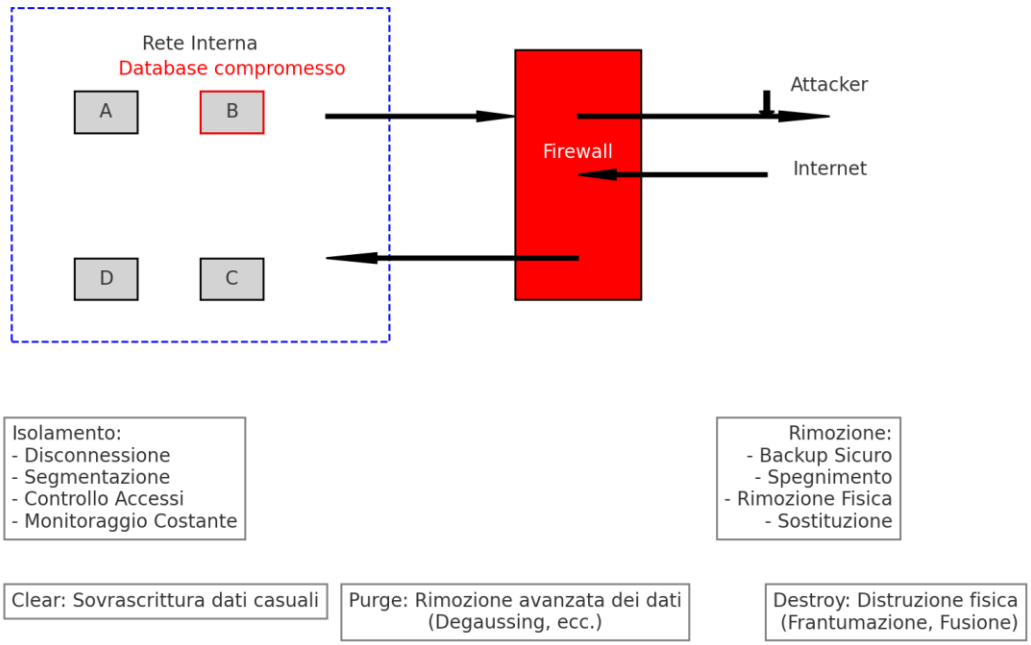
- **Clear**: Questo metodo implica la rimozione dei dati in modo che non possano essere recuperati tramite metodi standard di recupero dati. Un esempio è la sovrascrittura del disco con dati casuali. È meno sicuro rispetto agli altri due metodi ma può essere sufficiente in alcuni scenari.

- **Purge**: Si tratta di una rimozione più rigorosa dei dati, dove si adottano metodi avanzati per garantire che i dati non possano essere recuperati nemmeno con strumenti sofisticati di recupero. Questo può includere la degaussing (uso di forti campi magnetici) o altre tecniche che rendono i dati irrecuperabili.

- **Destroy**: Questo metodo comporta la distruzione fisica dei dispositivi di storage, come frantumare i dischi o fondere i componenti. Questo garantisce che i dati non possano essere recuperati in nessun modo, essendo il metodo più sicuro.

Procedura Suggerita

1. **Clear**: Iniziare con un processo di Clear per eliminare dati sensibili da dischi che devono essere riutilizzati.
2. **Purge**: Utilizzare Purge per i dischi che non possono essere facilmente distrutti ma che devono essere eliminati in sicurezza.
3. **Destroy**: Applicare Destroy per i dischi che contengono dati estremamente sensibili o che devono essere completamente eliminati senza possibilità di recupero.



Queste tecniche garantiscono che i dati sensibili siano trattati in modo adeguato, prevenendo ogni possibilità di recupero da parte di attaccanti o terzi non autorizzati.